



Subject	Date Last Reviewed	Policy #
Network Management Policy	October 2021	ITS-2.2
	Application	Supersedes
	ITS Security	ITS-2.1
	Distribution	
	All Departments	
Recommended	Approved	
 Preston D. Marx, VP Information Systems	 James I. Marshall, President & CEO	

1.0 Purpose

This policy defines the responsibilities and roles in relation to Uintah Basin Healthcare's network. It addresses general network security protocols including physical security, network design and personal responsibility.

2.0 Scope

The policy applies to the entire expanse of the Uintah Basin Healthcare network, including both wired and wireless networks in the organization. This includes owned properties as well as leased space when the UBH network has been extended.

3.0 Policy

Overview

Uintah Basin Healthcare's networks are essential to meet our mission and provide the services necessary for our success. In most cases, if the network fails work is affected and unwise workarounds ensue. We adhere to the CIA Triad model for network security: Confidentiality, Integrity and Availability. Solutions used by our organization, whether housed locally or in the cloud and their adjoining connectivity paths must maintain the CIA balance.

Network Support Responsibilities

Under the direction of the Vice President of Information Systems, the role of Network Administrator is assigned. The Network Administrator is technical by nature and is responsible for network installation, modification and design. They should have a detailed understanding of networking equipment and topographic design. The network administrator is expected to monitor and troubleshoot network traffic patterns, usage and threats.

Network Design

The Uintah Basin Healthcare network architecture is designed to optimize throughput and provides logical separation (segregation) of traffic. Traffic, whether internal or external, is managed through access controls to limit exposure and segmented appropriately. The LAN (Local Area Network) is designed for business use with these areas of emphasis:

- Physical Security – It is the responsibility of each UBH employee to assist in protecting our network. Unauthorized users should never be given access to UBH computers or other devices connected to the network. Where possible, access to network devices will be kept in a secure area.
- Corporate Firewall – Uintah Basin Healthcare's outside facing firewalls are housed locally, but are managed by Utah Telehealth Network. This firewall is in place to filter access to our private network and keep unauthorized or unwanted traffic out. VPN connections are utilized with business partners using at least 256-bit ciphers and the AES keys. An inventory of all network devices and connections will be kept current including circuit connections and VPN tunnels at each site.
- Endpoint Protection – As more services are web enabled and/or remote hosted, the endpoint becomes the perimeter. As such, an emphasis must be placed on: understanding the devices attached to the network, ensuring they are appropriately secure to communicate and access controls are in place to maintain least privileged access.

Security

The Network Administrator in cooperation with the entire ITS team, will utilize several tools and approaches to ensure proper network security.

- Regularly analyze and troubleshoot network traffic patterns
- Mitigate or eliminate weekly vulnerability threats found from Utah Telehealth Intrusion Prevention Systems and scans.
- Complete a penetration test annually and act upon any adverse findings.
- Keep all network devices on the latest stable IOS version.
- Ensure access, both physical and electronic, to network equipment is kept to a small authorized and knowledgeable group.
- At least monthly, share findings with management and mitigate or eliminate the risks as instructed.
- Access to solutions containing ePHI should be done in the most secure manner possible; avoiding the traversal of any public networks. Regardless of the network used, this traffic must be protected in transit through end-to-end encryption.

End Devices - Any endpoint device given access to the UBH internal network is subject to UBH policies and can be searched at any time to check for compliance. UBH purchased and managed equipment can be limited access, branded, managed and searched without notice.

Personal Devices

Personal electronic device use by employees is prohibited unless authorized for business purposes. Phones and other devices should be put away while at work and never attached to UBH networks. The private wired and wireless network is reserved for UBH devices doing company business. The public wireless network is for UBH visitors.

Violations

Uintah Basin Healthcare takes threats to their internal network seriously. Anyone found doing activities that are a threat to the network, create a hole in security or are circumventing UBH security measures will be subject to corrective action up to and including termination. If necessary, Uintah Basin Healthcare also reserves the right to advise appropriate legal officials of any illegal violations.